An Overview of Biometric Techniques

Garima Rani , Anshuman Saurabh
Department of Computer Engineering
SITE, Subharti University,Meerut,U.P. ,India

Abstract: **Biometric is basically a collection of methods for identification based on measuring the physiological characteristics that are unique to each and every person. It includes security of computer based systems ,e-banking, mobiles, laptops etc. With the use of biometrics it can be determine easily "who she/he is" rather then "what she/he has" (card, token, key) or "what she/he knows" (password, PIN). In this paper, We have discussed various biometric techniques.**

Keywords: **Biometrics, Multimodal Biometrics, Recognition, Verification, Identification, Security.**

1. INTRODUCTION

Biometric origins from the Greek words *bios* (life) and *metrikos* (measure). It is well known that humans intuitively use some body characteristics such as face, gait or voice to recognize each other. Since, today, a wide variety of applications require reliable verification schemes to confirm the identity of an individual, recognizing humans based on their body characteristics became more and more interesting in emerging technology applications. Traditionally, passwords and ID cards have been used to restrict access to secure systems but password and ID cards can be steel and are in convenient Biometric cannot be stolen, and forgetting of biometric is practically impossible.

2. BIOMETRIC TECHNIQUES

Biometric is a technique used to recognize the physical traits. Physical traits indicates various attributes of human body like as Voice, fingerprints, retinas and irises, voice template and hand measurements, for authentication purposes. A biometric technique based on a physiological characteristics is generally more reliable than one which adopts behavioural characteristics, even if the latter may be more easy to integrate within certain specific applications. In Biometric technique, A person can be recognized by using *verification and identification*. Verification confirms or deny a person's identity who (he or she) is claiming. It have one to one matching pattern. Identification is a comparison between various templates stored in database to a particular individual. It contain 1:N matching system. This implies that identification and verification are two problems that should be dealt with separately.

A biometric technique has four parts:

1) Sensor part, acquiring the biometric data,
2) Feature extraction part, with acquired data, extract feature vectors,
3) Matching part, feature vectors are ready to compare among acquired data,
4) Decision making part, whether a user login to a system with a valid ID or not.

For biometric techniques following requirements are needed:

1) Integrity should be maintained.
2) Uniqueness must be maintained.
3) Stability. It should be stable over lifetime.
4) Collectible it can be measured quantatively.

3. OVERVIEW OF COMMONLY USED BIOMETRICS

Since there are number of biometric methods in use (some commercial, some "not yet"), a brief overview of various biometric characteristics will be given, starting with newer technologies and then progressing to older ones:

Gait. This is one of the newer technologies and is yet to be researched in more detail. Basically, gait is the method of walking and it is a complex spatio-temporal biometrics. It is not fully distinctive but can be used in some lower security applications. Since video-sequence is used to measure several different movements this method is computationally expensive.

Hand geometry. In this technique, A user enter a pin code to claim his identity and then places hand on the system. Camera captured image of the hand. Thus silhouette of the hand is extracted and some geometrical properties are stored.

Fingerprint. A fingerprint is a combination of ridges and valleys. The ridges are the dark black area of fingerprint image and the valleys are the pure white area that exists between the ridges. Figure 1.1 shows an example of fingerprint image. The biological properties of fingerprint formation are well understood and fingerprints have been used for identification purposes from centuries. Fingerprint has been widely used for identification of criminals since 20th century. So most people do not feel comfortable in provide their fingerprints in many applications. Fingerprint-based authentication is very popular in a number of civilian and

commercial applications such as, welfare disbursement, cellular phone access, and laptop computer log-in due to its many advantages such that fingerprint based biometric system provide high degree of confidence in positive identification and also it can be embedded in various system (e.g., cellular phones).

Face. This technique uses an image or series of images either from a camera or photograph to recognize a person. The basic principle behind this techniques is analysis of the unique shape, pattern and positioning of facial features. Face recognition technique is still its early stage and many applications have been run on short database.

Retina. For a rational scan, there is a system used for reading a person's retina to scan the blood vessel pattern of a retina on the back side of the eyeball. This pattern is unique to every individual. A camera is used to project a beam inside the eye and capture the pattern and compare it to the reference file recorded previously known as template.

Iris. Iris recognition is another developed biometric recognition system capable of positively recognizing the identity of individuals without physical contact. The boundary of the pupil is defined by the video capture device, eyelid occlusion and specular reflection discounted, and the quality of the image is determined for processing. Iris patterns are processed and encoded, which are stored and used for future recognition transactions. Iris recognition usually takes only a second or two to complete and can accommodate both eyeglass and contact wearers. Indian Technologies, Inc. of Moorestown are based on iris recognition.

Iris scanning is one of the most accurate biometric user authentication techniques. High accuracy results from the fact that iris is very distinctive and rarely changes. The drawback is that the hardware employed is large and expensive. It requires user-training and controlled lighting.

Voice. In voice recognition system a person's voice is used to verify the identity of a person. In this system a person is verified and identified. A microphone on a standard PC with software is required for analyzing the unique characteristics of the person. This technique is mostly used in telephonic applications.

It is obvious that no single biometric is the "ultimate" recognition tool and the choice depends on the application. A brief comparison of the above techniques based on seven factors described in section 2 is provided in Table I.

Table I Comparison of various biometric technologies

Biometric characteristic	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Facial thermogram	H	H	L	H	M	H	L
Hand vein	M	M	M	M	M	M	L
Gait	M	L	L	H	L	H	M
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Ear	M	M	H	M	M	H	M
Hand geometry	M	M	M	H	M	M	M
Fingerprint	M	H	H	M	H	M	M
Face	H	L	M	H	L	H	H
Retina	H	H	M	L	H	L	L
Iris	H	H	H	M	H	L	L
Palmprint	M	H	H	M	H	M	M
Voice	M	L	L	M	L	H	H
Signature	L	L	L	H	L	H	H
DNA	H	H	H	L	H	L	L

4. PERFORMANCE OF BIOMETRIC SYSTEMS

Because of various positions on the acquiring sensor, imperfect imaging conditions, environmental changes, deformations, noise and bad user's interaction with the sensor, Biometric systems cannot handle that two patterns of the same biometric integrity, acquiring in different sessions, exactly collinear. On behalf of this reason a biometric matching systems' response is typically a matching score *s* that evaluate the closeness between the input numbers and the database pattern representations. A similarity score *s* is compared with an acceptance threshold *t* and if *s* is greater than or equal to *t* compared samples belong to a same person. Biometric samples (s) are different for different person and always less than t. If different persons generate scores from pair of samples is called imposter distribution, and if the same person generate scores from pair of samples is called genuine distribution.

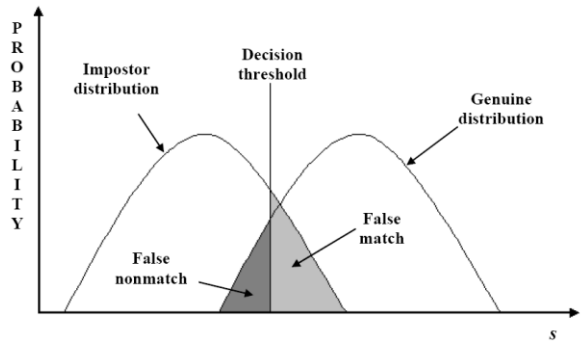

Figure I Biometric systems error rates

Following performance matrices are used to measure these errors:

- False match rate (FMR)- FMR measures the percentage of invalid inputs which are incorrectly matching the pattern.
- False non-match rate (FNMR)- FNMR measures the percentage of invalid inputs which are incorrectly rejected.

The basic functions of system threshold are FNMR and FMR. When system designer make the system more tolerant to input then the value of t decreases. By this FMR increase. For another condition, when system designer make the system more secure then the value of t increases. FMR and FNMR are brought together in a receiver operating characteristic (ROC) curve that plots the FMR against FNMR (or 1-FNMR) at different thresholds, Figure II.

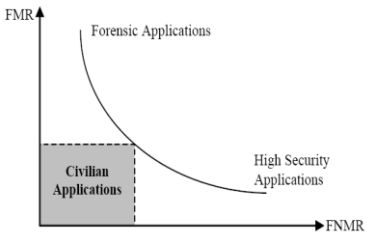

Figure II. Receiver operating characteristic (ROC)

- Failure to enrol rate (FTE) : FTE measures the percentage of low quality inputs which are not successful.
- Failure to capture rate (FTC) : FTC measured the correct input by which the system fails to deduct the input.

5. UNIMODAL BIOMETRIC TECHNIQUES

Biometric systems are being used for enhance security and reduction of financial frauds. Different biometric systems are being used for real time recognition. But some type of problems are not fully solved by the installed biometric systems.

Table II States of Error Rates closed with fingerprints, face, and voice biometric systems

Biometric characteristic	Test	Test Parameter	FNMR	FMR
Fingerprint	FVC2002 [3]	Users mostly in the age group 20-39	0.2 %	0.2 %
Face	FRVT2002 [5]	Enrollment and test images were collected in indoor environment and could be on different days	10 %	1 %
Voice	NIST2000	Text dependent	10-20 %	2-5 %

Single biometric properties have following limitations:

1. *Noise in sensed data*: Example is a fingerprint with a scare. Noisy data can also result from accumulation of dirt on a sensor or from ambient conditions.
2. *Inner class variations*: when individual authentication is vary at some other time and generate another pattern.
3. *Distinctiveness*: It leads large number of inner class variations with individual representation.
4. *Non-absoluteness*: When group of users have not universality properties. It means that similarity of users increases.

6. MULTIMODAL BIOMETRIC TECHNIQUES

Multi model techniques rectify all the problems of unimodal biometric techniques. Capturing different types of biometrics, multiple applications are used by multimodal biometric techniques. With the help of multi model, integration of biometric integrity and verification meet strict performance requirements. These models are more reliable than uni model. A multimodal techniques are the combination of face recognition and fingerprint verification, voice verification and smart-cards

Design of multimodal biometric techniques used in five integration scenarios: 1) *multiple sensors*, 2) *multiple biometrics*, 3) *multiple units of the same biometric*, 4) *multiple snapshots of the same biometric*, 5) *multiple representations for the same biometrics.*

7. CONCLUSION

In this paper we have provided a brief introduction of various biometric techniques. To sum up the above article is to bring out a complete and up-to-date review of published articles on biometric scenario is useful for the researchers of the field of biometric security systems. The presented work is very helpful for further study in the same field.

This study is carried out by the authors as we are working on a framework for biometrics security.

REFERENCES

[1] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", *IEEE Security & Privacy*, March/April 2003, pp. 33-42

[2] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 14, No. 1, pp 4-19, January 2004

[3] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, A. K. Jain, "FVC2002: Fingerprint verification competition" in *Proc. Int. Conf. Pattern Recognition (ICPR)*, Quebec City, QC, Canada, August 2002, pp. 744-747

[4] A. Ross, A. K. Jain, "Information fusion in biometrics", *Pattern Recognition Letters 24* (2003) 2115-2125, available at http://www.computerscienceweb.com/

[5] P. J. Philips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, J. M. Bone, "FRVT2002: Overview and Summary," available at: http://www.frvt.org/FRVT2002/documents.htm

[6] M. Golfarelli, D. Maio, D. Maltoni, "On the error-reject tradeoff in biometric verification systems," *IEEE Trans. Pattern Anal. Machine Intell.*, Vol. 19, pp. 786-796, July 1997

[7] J. Daugman, "How Iris Recognition Works", *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 14, No. 1, pp. 21-30, January 2004

[8] L. O'Gorman, "Seven issues with human authentication technologies," *in Proc. Workshop Automatic Identification Advanced Technologies (AutoID)*, Tarrytown, NY, Mar. 2002, pp. 185-186

[9] L. Hong, A. K. Jain, S. Pankanti, "Can multibiometrics improve performance?," in *Proc. AutoID'99, Summit*, NJ, October 1999, pp. 59-64

[10] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, R. P. W. Duin, "Is independence good for combining classifiers?," in *Proc. Int. Conf. Pattern Recognition (ICPR)*, Vol. 2, Barcelona, Spain, 2001, pp. 168-171

[11] L. Hong, A. K. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Trans. Pattern Analysis Machine Intell*., Vol. 20, pp. 1295-1307, December 1998

[12] A. K. Jain, A. Ross, "Multibiometric Systems", *Appeared in Communication of the ACM, Special Issue on Multimodal Interfaces*, Vol. 47, No.1, pp. 34-40, January 2004

[13] Boyce, A. Ross, M. Monaco, L. Hornak, and X. Li, "Multispectral iris analysis: a preliminary study," Proc. of IEEE Computer Society Workshop on Biometrics at CVPR, pp. 51-59, 2006.

[14] J. S. Pierrard and T. Vetter. Skin detail analysis for face recognition. In Proc. CVPR, pages 1–8, 2007.

[15] Usher, Y. Tosa, and M. Friedman, "Ocular biometrics: simultaneous capture and analysis of the retina and iris," Advances in Biometrics: Sensors, Algorithms and Systems, Springer Publishers, pp. 133-155, 2008.

[16] "Questions Raised About Iris Recognition Systems". *Science Daily*. 12 July 2012.

[17] Gelb, Alan; Julia Clark (2013). *Identification for Development: The Biometrics Revolution*. The Center for Global Development.

[18] Dr. Shubhamgi D C, Manohar Bali. ―Multi-Biometric Approaches to Face and Fingerprint Biometrics‖, International Journal of Engineering Research & Technology. 2278-0181. 2012.